Data Breach Management Policy

All users need to read, understand, and comply with this Policy

1. Introduction

1.1. The Company collects, holds, processes and shares large amounts of personal data and has an obligation to ensure that it is kept secure and appropriately protected.

1.2. Information is a key Company asset and as such ensuring the continued confidentiality, integrity and availability is essential to support the Company operations. The Company is also required to operate within the law, specifically the expectations set out in the Data Protection Act 1998 (DPA) and the General Data Protection Regulation (UK-GDPR).

1.3. Data security breaches are increasingly common occurrences whether these are caused through human or technical error or via malicious intent. As technology trends change and the volume of data and information created grows, there are more emerging ways by which data can be breached. The Company needs to have in place a robust and systematic process for responding to any reported potential data security breach, to ensure it can act responsibly, protect individual's data, Company information assets and reputation as far as possible.

1.4. Data security breaches will vary in impact and risk depending on the content and quantity of data involved, the circumstances of the loss and the speed of response to the incident. By managing all perceived data security breaches in a timely manner, it may be possible to contain and recover the data before it an actual breach occurs, reducing the risks and impact to both individuals and the Company. Breaches can result in fines for loss of personal information and significant reputational damage, and may require substantial time and resources to rectify the breach. As of May 2018, the GDPR replaced the DPA with fine limits increasing up to €20 million for a breach. Breach reporting within 72 hours of identifying a breach is mandatory under the GDPR, with fines of up to €10 million for failing to report a breach.

2. Purpose

2.1. The purpose of this procedure is to ensure that:

- personal data breaches are detected, reported, categorised and monitored consistently;
- incidents are assessed and responded to appropriately without undue delay;
- decisive action is taken to reduce the impact of a breach;
- improvements are implemented and communicated to prevent recurrence or future incidents;
- certain personal data breaches are reported to the Information Commissioner's Office (ICO) within 72 hours, where required.

2.2. This document sets out the procedure to be followed to ensure a consistent and effective approach in managing personal data security breaches across the Company.

3. Scope

3.1. This procedure applies to all staff, partner organisations and partner staff, suppliers, contractors, consultants, representatives and agents that work for or process, access, use or manage personal data on behalf of the Company.

3.2. This procedure relates to all personal and special category ('sensitive') information handled, stored, processed or shared by the Company whether organised and stored in physical or IT based record systems.

4. Definition

4.1. **What is a data security breach?**

- A personal data security breach means **"a breach of security leading to the loss, unauthorised destruction, alteration or disclosure of, or access to, personal data transmitted, stored or otherwise processed"**.
- A data security breach is considered to be any loss of, or unauthorised access to, Company data, normally involving Personal or Confidential information including intellectual property.
- Data security breaches include the loss, modification, or theft of data or equipment on which data is stored, inappropriate access controls allowing unauthorised use, human error (e.g. information sent to the incorrect recipient), hacking attacks and 'blagging' where information is obtained by deception.
- A personal data breach in the context of this procedure is an event or action that has affected the confidentiality, integrity or availability of personal data, either accidentally or deliberately, that results in its security being compromised, and has caused or has the potential to cause damage to the Company and/or the individuals to whom the information relates to.

4.2. **What is a data security incident?**

- A data security incident is where there is the risk of a breach but a loss or unauthorised access has not actually occurred.
- It is not always clear if an incident has resulted in a breach; by reporting all perceived data breaches quickly, steps can be taken to investigate, secure the information and prevent the incident becoming an actual breach (e.g. by reporting an email IT can remove the email before it has been read and therefore the data has been contained and not been seen by the incorrect recipient).
- For the purposes of this policy, data security breaches include both confirmed and suspected incidents and breaches.

4.3. **A data breach incident includes, but is not limited to:**

- Devices containing personal data being lost or stolen (e.g. laptop, USB stick, iPad/tablet device or paper record);
- Access by an unauthorised third party or unlawful disclosure of personal data to a third party Deliberate or accidental action (or inaction) by a data controller or processor;

- Sending personal data to an incorrect recipient;
- Alteration of personal data without permission;
- Loss of availability of personal data;
- Data input error / human error;
- Non-secure disposal of hardware or paperwork containing personal data;
- Inappropriate access/sharing allowing unauthorised use of, access to or modification of data or information systems;
- 'Blagging' offences where information is obtained by deceiving the organisation who holds it.

5. Reporting an Incident

5.1. The Company adopts a culture in which data protection breaches are reported. Any staff, contractor, partnership organisation, partner staff or individual that processes, accesses, uses or manages personal data on behalf of the Company is responsible for reporting information security incidents and data breaches immediately or within 24 hours of being aware of a breach to their supervisor or to the Legal Compliance Department at legal@top-magic.co.uk, who will investigate the potential breach.

5.2. If the breach occurs or is discovered outside normal working hours, it must be reported as soon as is practicable.

5.3. A Data Breach Report Form (see Appendix 1) should be completed as part of the reporting process and emailed it to their supervisor or to the Legal Compliance Department at legal@top-magic.co.uk. The report will include full and accurate details of the incident, when the breach occurred (dates and times), who is reporting it, the nature of the information and how many individuals are involved.

6. Containment & Recovery

6.1. The Legal Compliance Department in liaison with the respective supervisor and/or Information Security Officer, will determine if the breach is still occurring. If so, the appropriate steps will be taken immediately to minimise the effect of the breach.

6.2. An initial assessment will be made to establish the severity of the breach, who will take the lead as designated Investigating Officer to investigate the breach (this will depend on the nature of the breach) and determine the suitable course of action to be taken to ensure a resolution to the incident.

6.3. The Investigating Officer will establish whether there is anything that can be done to recover any losses and limit the damage the breach could cause.

6.4. The Investigating Officer will establish who may need to be notified as part of the initial containment.

6.5. Advice from experts across the Company such as IT, HR and legal and in some cases contact with external third parties may be sought in resolving the incident promptly.

7. Investigation & Assessing the Risks

7.1. An investigation will be undertaken by the Investigating Officer immediately and wherever possible within 24 hours of the breach being discovered/reported.

7.2. The Investigating Officer will investigate the breach and assess the risks associated with it, for example, the potential adverse consequences for individuals, how likely they are to happen and how serious or substantial they are.

7.3. The level of risk associated with a breach can vary depending on the type of data and its sensitivity.

7.4. The investigation will need to consider the following:

- What type of data is involved?
- How sensitive is the data?
- Where data has been lost or stolen are there any protections in place such as encryption?
- What has happened to the data? Has it been lost or stolen?
- Could the data be put to any illegal or inappropriate use?
- Could it be used for purposes which are harmful to the individuals to whom the data relates?
- How many individuals' personal data has been affected by the breach? Who are the individuals whose data has been breached?
- What harm can come to those individuals?
- Are there risks to physical safety or reputation, of financial loss or a combination of these and other aspects of their life?
- Are there wider consequences to consider?

8. Notification of Breaches

8.1. The Investigating Officer in consultation with the Legal Compliance Department and/or the Information Security Officer, will determine who needs to be notified of the breach.

8.2. Any notification must be agreed by the management.

8.3. Every incident will be assessed on a case-by-case basis.

8.4. Not every incident merit notification and over notification may cause disproportionate enquiries and work.

8.5. The following will need to be considered:

- Are there any legal/contractual notification requirements?
- Can notification help the individual? Could they take steps to act on the information to protect themselves?
- Would notification help prevent the unauthorised or unlawful use of personal data?
- Can notification help the Company meet its obligations under the data protection principles?
- Is there a large number of people that are affected? Are there serious consequences?

- Should the ICO be notified of the personal data breach? The ICO must be notified where there is likely to be a risk to people's rights and freedoms.
- If so, notification shall be within 72 hours with details of:
  a) a description of the nature of the personal data breach including, where possible:
     - the categories and approximate number of individuals concerned; and
     - the categories and approximate number of personal data records concerned.
  b) the name and contact details of the data protection officer or other contact point where more information can be obtained;
  c) a description of the likely consequences of the personal data breach;
  d) details of the security measures and procedures in place at the time the breach occurred; and
  e) a description of the measures taken, or proposed to be taken, to deal with the personal data breach, including, where appropriate, the measures taken to mitigate any possible adverse effects.

8.6. If a breach is likely to result in a high risk to the rights and freedoms of individuals, notification to the individuals whose personal data has been affected by the incident must be without undue delay describing:

- the nature of the personal data breach;
- the name and contact details of the data protection officer or other contact point where more information can be obtained;
- a description of the likely consequences of the personal data breach; and
- a description of the measures taken, or proposed to be taken, to deal with the personal data breach and including, where appropriate, of the measures taken to mitigate any possible adverse effects including what action the individual(s) can take to protect themselves.
- The following factors to consider include:
- Sensitivity of information;
- Volume of information;
- Likelihood of unauthorised use;
- Impact on individual(s);
- Feasibility of contacting individuals.

8.7. If the Company decides not to notify the individuals affected, it will still need to notify the ICO unless it can demonstrate that the breach is unlikely to result in a risk to rights and freedoms.

8.8. The Investigating Officer and/or Legal Compliance Department must consider notifying third parties such as the police, insurers, professional bodies, bank or credit card companies who can help reduce the risk of financial loss to individuals. This would be appropriate where illegal activity is known or is believed to have occurred, or where there is a risk that illegal activity might occur in the future.

8.9. The Investigating Officer and/or Legal Compliance Department will consider whether the Marketing and Communications Team should be informed regarding a press release and to be ready to handle any incoming press enquiries.

8.10. All personal data breaches and actions will be recorded by the Legal Compliance Department regardless of whether or not they need to be reported to the ICO.

9. Evaluation & Response

9.1. Data protection breach management is a process of continual review. Once the initial incident is contained, the Investigating Officer will carry out a full review of the causes of the breach; the effectiveness of the response(s) and whether any changes to systems, policies and procedures should be undertaken.

9.2. Existing controls will be reviewed to determine their adequacy, and whether any corrective action should be taken to minimise the risk of similar incidents occurring.

9.3. The review will consider:

- Where and how personal data is held/ stored;
- Where the biggest risks lie and identify any further potential weak points within its existing security measures;
- Whether methods of transmission are secure;
- Sharing minimum amount of data necessary;
- Staff awareness.

9.4. Regardless of the type and severity of incident, there will always be recommendations to be made even if it is only to reinforce existing procedures.

9.5. All recommendations will be assigned an owner and have a timescale by when they should be implemented which has a dual purpose. The first is to ensure that the Company puts in place whatever measures have been identified and that there is an individual that can report back to the Investigating Officer on progress. The second is that where incidents are reported to the ICO, the Company can demonstrate that the measures have either been put in place or that there is a documented plan to do so.

9.6. Identifying recommendations is more than just damage control. The knowledge of what has happened together with the impact is a fundamental part of learning and continual improvement which can then be disseminated throughout the Company.

Last Updated: 05 February 2026